18. Configuring IGMP Snooping

This section describes Internet Group Management Protocol (IGMP) snooping concepts and how to configure the Tellabs 8800 series MSR to perform IGMP snooping:

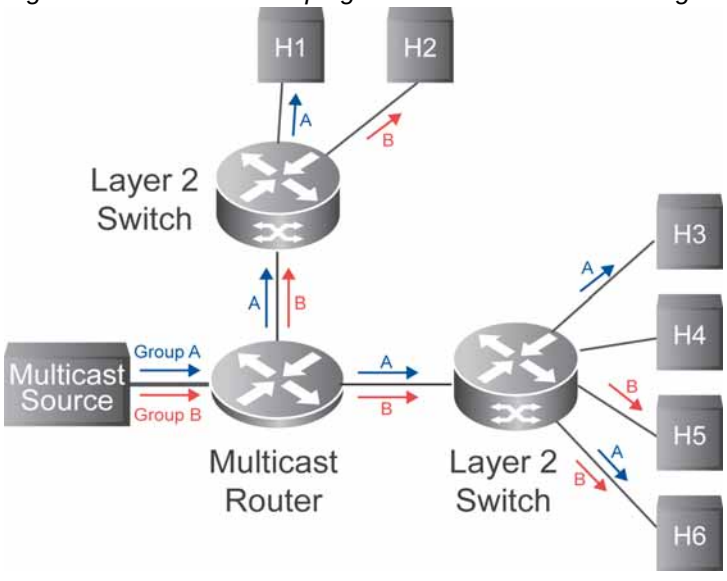
- About IGMP Snooping, page 4-359
- About IGMP Snooping Configuration, page 4-363
- IGMP Snooping Configuration Examples, page 4-367

About IGMP Snooping

The IGMP snooping protocol allows a Layer 2 switch to selectively forward IP multicast traffic only to hosts and routers processing that traffic.

An IGMP snooping-enabled Layer 2 switch inspects (snoops) headers of IGMP protocol messages transmitted between hosts and routers. The switch uses the header information to selectively forward multicast packets only to those interfaces where hosts are members of a chosen multicast group. Figure 18.1, page 4-359 shows an example of IGMP snooping. In this example, only hosts with membership in Group A receive Group A multicast traffic and only hosts with Group B membership receive Group B multicast traffic. If a host is not a group member, no multicast traffic is forwarded. This contrasts with the typical Layer 2 forwarding behavior of flooding multicast traffic to all other interfaces on a network.

Figure 18.1 IGMP Snooping Multicast Traffic Forwarding



The benefit of IGMP snooping is bandwidth conservation. Without IGMP snooping, the Layer 2 switches copy and forward incoming multicast packets to all other interfaces in the same network. This mode of multicasting consumes significant bandwidth.

The Tellabs 8800 series MSR with IGMP snooping provides the following bandwidth conservation advantages:

- Prevents sending multicast traffic to hosts that are not members of the multicast group.
- Performs some IGMP message management tasks normally done by the multicast router. This is known as IGMP proxy. Refer to IGMP Snooping on the Tellabs 8800 Series MSR, page 4-361 for IGMP snooping functions performed by the Tellabs 8800 series MSR.

The Tellabs 8800 series MSR supports IGMP snooping for IGMPv1 and IGMPv2 protocols. For IGMPv1 and IGMPv2 standards, refer to Supported Standards, page 4-779.

IGMP snooping on the Tellabs 8800 series MSR operates in a Virtual Private LAN Service (VPLS) network. For details about VPLS, refer to the *TMOS VPLS Application Manual, 76.8800FP801/28*.

For details about how IGMP snooping operates with VPLS, refer to IGMP Snooping on the Tellabs 8800 Series MSR, page 4-361.

The following topics describe the IGMP snooping protocol:

- IGMP Snooping Terminology, page 4-360
- IGMP Snooping on the Tellabs 8800 Series MSR, page 4-361

IGMP Snooping Terminology

The following section describes terms related to IGMP snooping on the Tellabs 8800 series MSR.

IGMP

Internet Group Management Protocol (IGMP) is a communications protocol for managing the membership of IP multicast groups. IP hosts use IGMP to report multicast group memberships to neighboring multicast routers. Multicast routers use IGMP to learn which groups have members on each of the attached networks. A multicast router keeps a list of multicast group memberships for each attached network, and a timer for each membership.

Refer to Configuring IP Multicasting, page 4-339 for details about IGMP.

IGMP Messages

IGMP provides three types of protocol messages used in the host-router exchange.

- Query. Queries determine group memberships. A multicast router sends queries to determine which multicast addresses are of interest to hosts. There are two types of queries, general and group-specific:
  - General query. A multicast router periodically sends a general query, 224.0.0.1, to refresh the group memberships.
  - Group-specific query. A multicast router sends a group-specific query for a particular IP multicast address to learn whether a group has any members on an attached network.
- Membership report. A host sends a membership report, also referred to as a join, or report, to join a group. By sending a report, the host expresses interest in receiving packets from a particular multicast group address.

- Leave Group. A leave group message, or leave, applies to IGMPv2 hosts. An IGMPv2 host sends a leave to stop receiving packets for a specific multicast group address. With IGMPv1, a host leaves by not responding to periodic general queries. This is known as a silent leave.

IP Multicasting

IP multicasting is the transmission of IP data packets to a host group. Refer to Configuring IP Multicasting, page 4-339 for details about IP multicasting.

Host

A host is a customer edge (CE) device that receives multicast traffic by joining a multicast group membership. A host joins a multicast group by either:

- sending an unsolicited membership report for a specific IP multicast group, or
- responding to a general query with a membership report.

Group

A group is a set of zero or more hosts identified by a single IP destination address.

Membership in a group is dynamic. Hosts may join or leave a group at any time. A host may be a member of more than one group at a time.

Class D IP addresses, in the range of 224.0.0.0 to 239.255.255.255, identify host groups. The address 224.0.0.0 is not assigned to any group. 224.0.0.1 is permanently assigned and used to address all multicast hosts as a general query. Refer to IPv4 Multicast Addresses, page 4-340 for details.

Multicast

Multicast is the abbreviated term for IP multicast, which is a one-to-many communication protocol over an IP network. Multicast messages originate from a single device, while multiple devices around the network may receive that same multicast message.

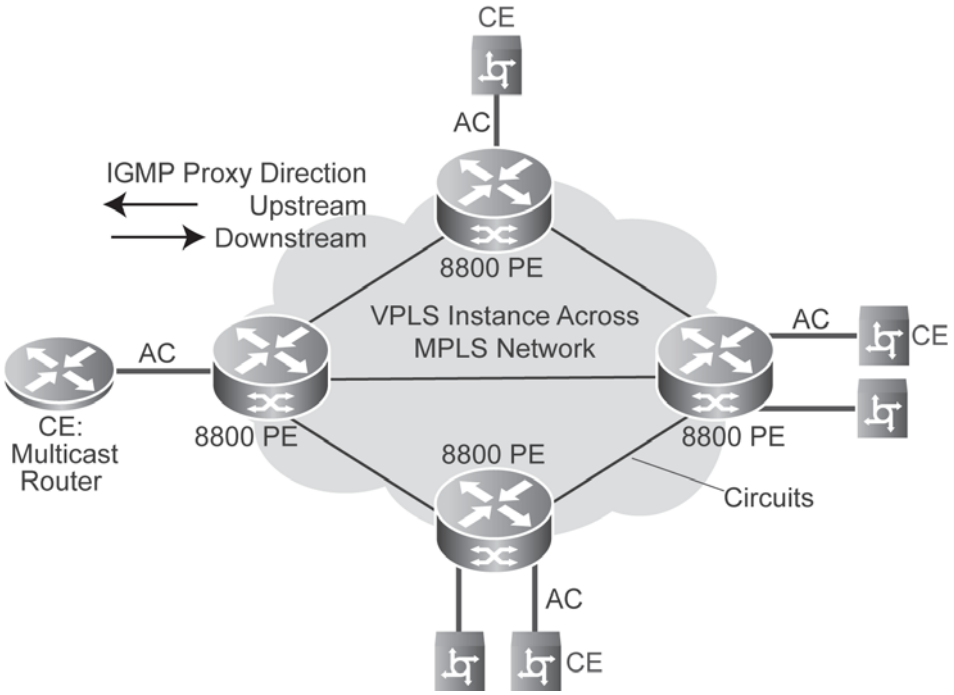
Multicast Router

A multicast router is a customer-edge (CE) device that transmits IP multicast packets to other networks that have members of a destination group. A multicast router keeps a list of multicast group memberships for each network, and a timer for each membership.

IGMP Snooping on the Tellabs 8800 Series MSR

The Tellabs 8800 series MSR performs IGMP snooping on IGMPv1 and IGMPv2 multicast traffic transmitted across a Virtual Private Lan Service (VPLS). VPLS is an Ethernet-based bridge domain that bridges traffic among geographically distributed CE sites in an MPLS network. Figure 18.2, page 4-362 shows the role of Tellabs 8800 series MSRs in a VPLS topology transporting multicast traffic.

Figure 18.2 VPLS Topology Set Up for IGMP Snooping



With VPLS, the Tellabs 8800 series MSR is a provider edge (PE) node connected to CE devices via attachment circuits (ACs). Pseudowire (PW) circuits originate from PEs and connect across an MPLS network to other PEs. When PEs are assigned to a specific VPLS instance, the connected CEs appear to be part of a single LAN.

Refer to the *TMOS VPLS Application Manual, 76.8800FP801/28*, for more details about VPLS.

CEs function as either multicast routers or hosts. The multicast router transmits multicast traffic to the ingress port of the PE; the PE replicates and forwards the traffic out the other ports. The multicast router continues to forward multicast traffic through the VPLS as long as one or more hosts respond to periodic IGMP queries. The multicast router can be either statically configured or discovered automatically through the general query process.

With IGMP snooping, the PE snoops multicast packets and builds forwarding tables based on multicast group addresses and corresponding interfaces. When a PE receives multicast packets for a given group from the CE router, the PE performs a lookup and forwards the packets only to those interfaces with CEs that are members of the multicast group.

When the MSR receives a join from a host, the MSR adds the interface and group address to the forwarding table, and forwards the report to the multicast router. When the MSR receives a leave from a host, the MSR removes the host from the forwarding table and forwards the leave to the multicast router.

IGMP Proxy

In a VPLS network, the Tellabs 8800 series MSR is capable of IGMP snooping with proxy functionality, also referred to as IGMP proxy. Network traffic flow is a factor in IGMP proxy; traffic flow toward the multicast router is the upstream direction, traffic flow toward the host is the downstream direction. Figure 18.2, page 4-362 shows network traffic flow direction for IGMP proxy.

IGMP proxy reduces message traffic on the network as the MSR performs some multicast router functions downstream toward the host, and some host management functions upstream toward the multicast router. IGMP proxy functionality includes the following:

- Query response. With IGMP proxy, the MSR receives the query from the multicast router and performs a lookup for the group address. If the forwarding table contains the group address, the MSR responds by forwarding a membership report as a proxy for the hosts.

  The MSR also responds to a query as a backup to a host, when a host loses connection, and cannot send a leave, or when an interface connected to the host goes down, for example.
- Message consolidation. The MSR consolidates both leave and report messages before forwarding upstream to the multicast router.

  When a host leaves a group, the MSR checks the forwarding table for other hosts that are still members of that group. The MSR forwards the leave when no other hosts remain in the group.

  If the MSR sends a report upstream to the multicast router, subsequent reports for the same group are not sent upstream.
- Fast reporting. Fast reporting is an unsolicited reporting mechanism to immediately alert upstream interfaces that a new host has joined a group. The MSR calculates a fast reporting interval from the configured robustness value at the configured maximum response interval. Refer to Robustness, page 4-366 for details.
- Fast network convergence. The Tellabs 8800 series MSR performs proxy queries for fast network convergence. When an AC on an interface or circuit becomes operational, the MSR sends an IGMP general query to obtain group membership information.

About IGMP Snooping Configuration

The following topics describe IGMP snooping configuration:

- Configuration Guidelines, page 4-363
- IGMP Snooping Parameters for the VPLS Bridging Instance, page 4-364
- IGMP Snooping Parameters for the VPLS Interface and Circuit, page 4-366

Configuration Guidelines

IGMP snooping operates on the Tellabs 8800 series MSR within the bridging context of a VPLS network. The following guidelines apply for IGMP snooping on the MSR:

- After an upgrade to FP8.0.1, the Tellabs 8800 series MSR comes up with IGMP snooping disabled on all bridging instances. When enabled, the IGMP snooping parameters on a VPLS bridge, interface, or circuit that govern IGMP snooping are at default values.

- After establishing VPLS, IGMP snooping configuration and operations apply only to VPLS bridging instances, VPLS bridging interfaces, and VPLS bridging circuits.
- IRB bridging instances do not support IGMP snooping.
- You must configure MPLS and a VPLS bridging instance before configuring IGMP snooping on an MSR. Refer to the *Tellabs TMOS VPLS Application Manual, 76.8800FP801/28*, for details.

IGMP Snooping Parameters for the VPLS Bridging Instance

You can customize IGMP snooping on your VPLS network by using the Tellabs 8800 series MSR TMOS CLI command, **enable config bridging-instance protocol igmp-snooping**, to configure various IGMP snooping parameters.

The following CLI help string displays configurable IGMP snooping commands.

```
8860# enable config bridging-instance protocol igmp-snooping ?

 admin                - Set igmp snooping admin state
 group-exp-timer      - Set igmp snooping group expiration timer
 immediate-leave      - Set igmp snooping immediate leave state
 last-mem-qry-interval
                      - Set igmp snooping last member query interval
 max-response-time    - Set igmp snooping max response time
 mrouter-exp-timer    - Set igmp snooping multicast-router expiration timer
 query                - Set igmp snooping action for general query
 query-time-interval  - Set igmp snooping query time interval
 robustness           - Set igmp snooping robustness
 source-ip            - Set source IP address for generating queries
 unknown-group        - Set igmp snooping action for unknown group query
```

The following IGMP snooping parameters are configurable for a VPLS bridging instance:

- Group Expiration Time, page 4-364
- Immediate Leave, page 4-365
- Last Member Query Interval, page 4-365
- Maximum Response Time, page 4-365
- Multicast Router Expiration Timer, page 4-365
- Multicast Router Address, page 4-365
- Query, page 4-366
- Query Time Interval, page 4-366
- Robustness, page 4-366
- Unknown Group, page 4-366

Group Expiration Time

The group expiration time parameter, **group-exp-timer**, is the time that a Tellabs 8800 series MSR waits to receive a group membership report before deleting the multicast group address from the multicast forwarding table.

When the MSR detects a multicast group, the MSR adds the group address to the forwarding table and sets the group expiration timer. If the MSR does not detect a membership report for that group within the group expiration time, the MSR removes the group from the forwarding table.

The range is 130–65,535 seconds. The default is 260 seconds.

Immediate Leave	The immediate leave, or fast leave parameter, **immediate-leave**, is an IGMPv2 setting that determines whether a Tellabs 8800 series MSR performs host leave processing. When enabled, the MSR drops the group from the host as soon as a leave report is received; the MSR does not perform leave processing. With **immediate-leave** disabled, the MSR performs leave processing when the MSR receives a leave report from a host. You can set **immediate-leave** to *enable* or *disable*. The default value is *enable*.
Last Member Query Interval	The last member query interval, **last-mem-qry-interval**, is the query cycle time for host leave processing. In the host leave process, the Tellabs 8800 series MSR sends a group-specific query to a host. If there is no response within the query cycle, the MSR re-sends the group-specific query and waits for a response. This querying process repeats for the configured robustness count. If the MSR does not receive a response, the MSR removes the host from the multicast forwarding table group membership. The range is 1–255 tenths of a second. The default value is 10 tenths of a second (1 second).
Maximum Response Time	The maximum response time, **max-response-time**, is the maximum time to wait for a host response to a general query. The Tellabs 8800 series MSR randomly selects a delay time between zero and the maximum response time before sending consolidated reports upstream in response to a general query. In addition, the MSR uses maximum response time in conjunction with robustness count to perform fast reporting. Fast reporting is a mechanism for sending unsolicited reports upstream. Fast reporting is sent using the robustness count at the interval of maximum response time. The range is 10–65,535 tenths of a second. The default value is 100 tenths of a second (10 seconds).
Multicast Router Address	Configure the **source-ip** parameter, when IGMP proxy needs to generate a query with a valid source IP address. If the multicast router IP address is not set, the Tellabs 8800 series MSR node acts as an IGMP proxy for the multicast router, and displays 0.0.0.0. Use this parameter to assign a source IP address when a CE does not accept a **source-ip** of 0.0.0.0. The format is dotted decimal, a.b.c.d. The default value is 0.0.0.0.
Multicast Router Expiration Timer	The **mrouter-exp-timer**, is the time that a Tellabs 8800 series MSR waits before deleting a multicast router from the routing table. When the node dynamically learns a multicast router address, the node sets the multicast router expiration timer. If the node does not detect a query within the elapsed time, the node removes the multicast router. The range is 130–65,535 seconds. The default value is 400 seconds.

Query

The **query** parameter governs how the Tellabs 8800 series MSR manages queries on downstream interfaces.

You can set **query** to *forward* or *generate*. The default value is *forward*.

When the **query** action is *forward*, the node forwards (floods) to all downstream interfaces when it receives a query from the multicast router interface.

When this parameter is set to *generate*, the MSR manages each downstream interface individually. As each interface becomes operationally up, the MSR generates an immediate query on the downstream interface, independent of the multicast router. The MSR also applies the query time interval to generate subsequent queries for the downstream interface.

Query Time Interval

The parameter, **query-time-interval**, is the time interval that a Tellabs 8800 series MSR applies when generating periodic queries on downstream interfaces. The range is 60 – 65,535 seconds. The default value is 125 seconds.

Robustness

The **robustness** multiplier is a parameter that determines the number of times the Tellabs 8800 series MSR sends a fast report or performs the host leave process.

The range is 1–255. The default value is 2.

Unknown Group

The **unknown-group** parameter determines how a Tellabs 8800 series MSR processes an unfamiliar multicast group address in the downstream direction. An unknown group is a multicast IP address not learned by the node, and therefore, not in the multicast forwarding table.

You can set **unknown-group** to *drop* or *forward*. The default value is drop.

When set to *drop*, the node drops unknown group traffic.

When set to *forward*, the MSR forwards all unknown groups downstream.

IGMP Snooping Parameters for the VPLS Interface and Circuit

You can configure IGMP snooping parameters for an individual VPLS interface or circuit in a VPLS network.

The following CLI help strings display configurable IGMP snooping parameters for the interface and circuit.

```
8860# enable config interface ge-1/8/2/1.1 protocol igmp-snooping ?

 immediate-leave      - Set immediate leave state for Interface
 mrouter              - Set igmp snooping multicast-router version
 [no] static-group    - Set igmp snooping static group address?

8860# enable config ckt name pe1-to-pe3 protocol igmp-snooping ?

 immediate-leave      - Set igmp snooping immediate leave state
 mrouter              - Set igmp snooping multicast-router version
 [no] static-group    - Set igmp snooping static group address
```

The following topics describe configurable IGMP snooping parameters for the VPLS interface and circuit:

- IGMP Multicast Version, page 4-367
- Immediate Leave, page 4-367
- Static Multicast Address, page 4-367

IGMP Multicast Version

The **mrouter** parameter allows you to set the multicast router version on an interface or circuit. The settings are *v1*, *v2*, or *disable*. The default is *disable*.

Immediate Leave

The **immediate-leave** parameter on a VPLS interface has the same functionality as on the VPLS bridging instance described in IGMP Snooping Parameters for the VPLS Bridging Instance, page 4-364.

When configured on the interface or circuit, the immediate leave setting overrides the VPLS bridging instance setting on a VPLS interface or a VPLS circuit. You can set the value to enable or disable. The default value is enable.

Static Multicast Address

The **static-group** parameter sets a static Class D IP address on an interface or circuit. You can add a static group or delete a static group.

IGMP Snooping Configuration Examples

The following configuration examples implement IGMP snooping on a VPLS network:

- Enabling IGMP Snooping on a VPLS Bridging Instance, page 4-367
- Configuring IGMP Snooping on a VPLS Interface, page 4-368
- Configuring IGMP Snooping on a VPLS Circuit, page 4-371

Enabling IGMP Snooping on a VPLS Bridging Instance

Refer to Figure 18.3, page 4-367 for an example of VPLS topology for configuring IGMP snooping on a bridging instance.

Figure 18.3 IGMP Snooping Configuration on VPLS

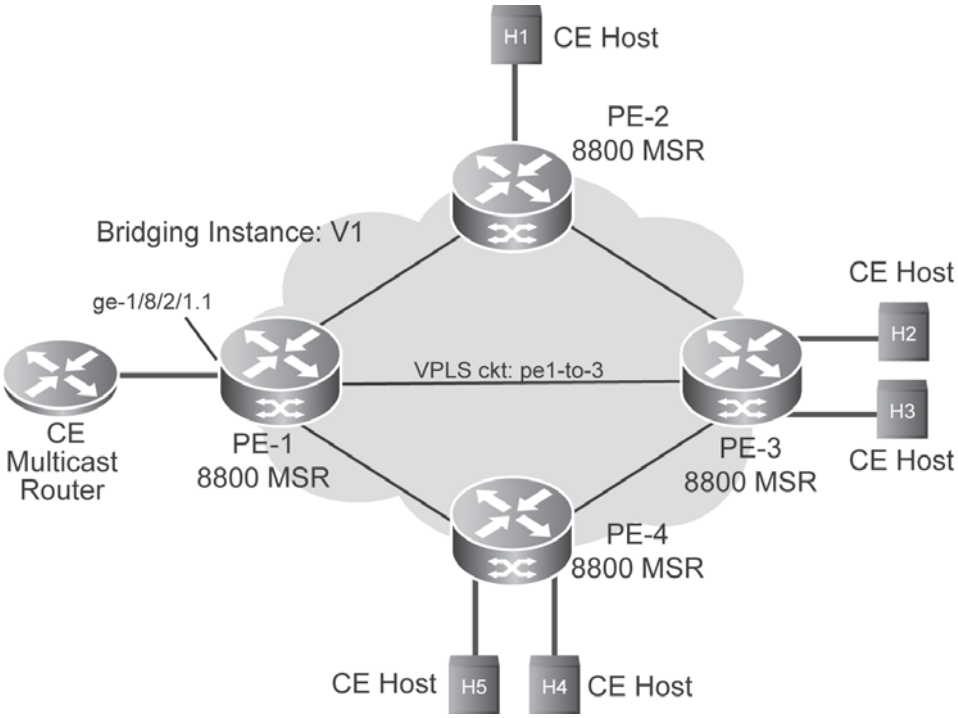


Table 18.1, page 4-368, lists and describes the steps for enabling IGMP snooping on a VPLS bridging instance. This configuration example assumes that you have created a VPLS bridging instance named *v1*.

Table 18.1 Configuring IGMP Snooping on a VPLS Bridging Instance

	Command Entry	Purpose
Step 1.	`8800# enable config`	Enter the configuration mode.
Step 2.	`8800(config)# bridging-instance name v1 protocol igmp-snooping admin enable`	Enable IGMP snooping on the VPLS bridging instance, v1. When enabled, default values are set.
Step 3.	`8800(config)# exit`	Exit configuration mode.
Step 4.	`8800# show bridging-instance name v1 protocol igmp-snooping`	Display IGMP snooping for the bridging instance.

Displaying IGMP Snooping on a VPLS Bridging Instance

Use the **show bridging-instance protocol igmp-snooping** command to display the IGMP snooping on a VPLS bridging instance.

```
8800# show bridging-instance name v1 protocol igmp-snooping

Tellabs8840# show bridging-instance name v1 protocol igmp-snooping

Bridge Instance      Admin      OperSts    Group Count
---------------      -------    -------    -----------
v1                   enable     up         1

8800# show bridging-instance name v1 protocol igmp-snooping extensive

Bridge Instance: v1 (Id: 1)
  Admin State: enable; Operational Status: up; Failure Reason: none
  Generate Query Action: generate query; Unknown Group Action: drop
  Immediate Leave: enable; Query Time Interval: 125 (sec)
  Last Member Query Interval: 10 (100ms); Max Response Timer: 100 (100 ms)
  Last Group Clear Time: not available; MRouter Expiry Time: 400 (sec)
  Group Expiry Timer: 260 (sec); Robustness: 2; Group Count: 1
  Source IP: 0.0.0.0; IGMP Version: v2
  MRouter Interface Count: 1

  MRouter Interface / Ckt Name
  ----------------------------
  ge-1/8/2/1.1

Statistics Information:
  Category               Count      Category               Count
  --------               -------    --------               -------
  Tx General Query       9677       Rx General Query       4950
  Tx Group Spec Query    0          Rx Group Spec Query    0
  Tx V1 Report           0          Rx V1 Report           0
  Tx V2 Report           4950       Rx V2 Report           4874
  Tx Group Leave         0          Rx Group Leave         0
  Tx Unknown Type        0          Rx Unknown Type        0
                                    Rx Error Packet        0
                                    Rx Drop Packet         0
```

Configuring IGMP Snooping on a VPLS Interface

Before you configure an IGMP snooping parameter on a VPLS interface, you must have enabled IGMP snooping on the VPLS bridging instance.

If required, refer to one or more of the following procedures to configure IGMP snooping on a bridging sub-interface.

- Configuring IGMP Snooping Immediate-Leave on a VPLS Interface, page 4-369
- Configuring the IGMP Snooping Multicast Router Version for a VPLS Interface, page 4-369

- Configuring an IGMP Snooping Static Group on a VPLS Interface, page 4-369

Refer to Figure 18.3, page 4-367 for a VPLS topology example for configuring IGMP snooping.

Configuring IGMP Snooping Immediate-Leave on a VPLS Interface

Table 18.2, page 4-369, lists the CLI commands to configure immediate-leave on an IGMP snooping interface.

Table 18.2 Configuring IGMP Snooping Immediate-Leave on a VPLS Interface

	Command Entry	Purpose
Step 1.	`8800# enable config`	Enter the configuration mode.
Step 2.	`8800(config)# interface ge-1/8/2/1.1 protocol igmp-snooping immediate-leave disable`	Set immediate-leave action on a selected interface. Setting this interface attribute overrides the immediate-leave action on bridging instance. The default is enable.
Step 3.	`8800(config)# exit`	Exit configuration mode.
Step 4.	`8800 # show interface ge-1/8/2/1.1 protocol igmp-snooping extensive`	Display IGMP snooping configuration for the interface.

Configuring the IGMP Snooping Multicast Router Version for a VPLS Interface

Table 18.3, page 4-369, lists the CLI commands to set the IGMP snooping multicast router IGMP version for a VPLS interface.

Table 18.3 Configuring the IGMP Snooping Multicast Router Version on a VPLS Interface

	Command Entry	Purpose
Step 1.	`8800# enable config`	Enter the configuration mode.
Step 2.	`8800(config)# config interface ge-1/8/2/1.1 protocol igmp-snooping mrouter v2`	Defines the multicast router IGMP version on an interface.
Step 3.	`8800(config)# exit`	Exit configuration mode.
Step 4.	`8800 # show interface ge-1/8/2/1.1 protocol igmp-snooping extensive`	Display IGMP snooping configuration for the VPLS interface.

Configuring an IGMP Snooping Static Group on a VPLS Interface

Table 18.4, page 4-369, lists the CLI commands to add or delete an IGMP snooping multicast group to a VPLS interface.

Table 18.4 Configuring an IGMP Snooping Static Group on a VPLS Interface

	Command Entry	Purpose
Step 1.	`8800# enable config`	Enter the configuration mode.

Table 18.4 Configuring an IGMP Snooping Static Group on a VPLS Interface (Continued)

	Command Entry	Purpose
Step 2.	8800(config)# **config interface** *ge-1/8/2/1.1* **protocol igmp-snooping static-group** *239.0.0.1* 8800(config)# **config interface** *ge-1/8/2/1.1* **protocol igmp-snooping no static-group** *239.0.0.1*	Adds a multicast group (non-local class D IP address) to an interface. OR Deletes a multicast group (non-local class D IP address) from an interface.
Step 3.	8800(config)# **exit**	Exit configuration mode.
Step 4.	8800 # **show interface** *ge-1/8/2/1.1* **protocol igmp-snooping** *detail*	Display IGMP snooping configuration for the VPLS interface.

Displaying IGMP Snooping on a VPLS Interface

Use the **show interface protocol igmp-snooping** command to display IGMP snooping parameters for an interface.

```
8800# show interface ge-1/8/2/1.1 protocol igmp-snooping
                                    Op          Imm  Static Total
Interface        Bridge Instance    St   MRtr   Lve  Group  Group
---------------- ---------------- ---  ----  ---  -----  -----
ge-1/8/2/1.1     v1                 up   V2    en   1      1

8800# show interface ge-1/8/2/1.1 protocol igmp-snooping detail

Interface: ge-1/8/2/1.1; Bridging Instance: v1
  Admin State: enable; Oper Status: up; Failure Reason: none
  Immediate Leave: enable; MRouter: V2
  Total Groups: 1; Static Groups: 1
  Last Group Clear Time: not available; MRouter Type: static; Rem Time: 0
```

Use the **show interface protocol igmp-snooping groups all** command to display the static groups assigned to an IGMP snooping interface.

```
8800# show interface ge-1/8/2/1.1 protocol igmp-snooping groups all

Interface        Group Addr       Ver  Type  Remain         Last Reporter
-------------    -------------    ---  ----- ------------   -------------
ge-1/8/2/1.1     224.30.30.30     V2   Sta   0              n/a
```

Use the **show interface protocol igmp-snooping statistics** command to display statistics for an IGMP snooping interface.

```
8800# show interface ge-1/8/2/1.1 protocol igmp-snooping statistics

Interface: ge-1/8/2/1.1

Statistics Information:
  Category               Count      Category               Count
  --------               -------    --------               -------
  Tx General Query       24         Rx General Query       5004
  Tx Group Spec Query    0          Rx Group Spec Query    0
  Tx V1 Report           0          Rx V1 Report           0
  Tx V2 Report           5006       Rx V2 Report           48
  Tx Group Leave         0          Rx Group Leave         0
  Tx Unknown Type        0          Rx Unknown Type        0
                                    Rx Error Packet        0
                                    Rx Drop Packet         0
```

Configuring IGMP Snooping on a VPLS Circuit

Before you configure an IGMP snooping parameter on a VPLS circuit, you must have configured IGMP snooping on the VPLS bridging instance.

If required, refer to one or more of the following procedures to configure IGMP snooping on a VPLS circuit.

- Configuring IGMP Snooping Immediate-Leave for a Circuit, page 4-371
- Configuring the IGMP Snooping Multicast Router Version for a Circuit, page 4-371
- Configuring an IGMP Snooping Static Group on a Circuit, page 4-372

Figure 18.3, page 4-367 is a VPLS topology example for configuring IGMP snooping.

Configuring IGMP Snooping Immediate-Leave for a Circuit

Table 18.5, page 4-371, lists the CLI commands to configure IGMP snooping for a circuit.

Table 18.5 Configuring IGMP Snooping Immediate-Leave on a Circuit

	Command Entry	Purpose
Step 1.	`8800# enable config`	Enter the configuration mode.
Step 2.	`8800(config)# ckt name pe1-to-pe3 protocol igmp-snooping immediate-leave disable`	Set immediate-leave action on a selected circuit. Setting this interface attribute overrides the immediate-leave action on bridging instance. The default is enable.
Step 3.	`8800(config)# exit`	Exit configuration mode for bridge v1.
Step 4.	`8800 # show ckt name pe1-to-pe3 protocol igmp-snooping extensive`	Display IGMP snooping configuration for the circuit.

Configuring the IGMP Snooping Multicast Router Version for a Circuit

Table 18.6, page 4-371, lists the CLI commands to set the IGMP Snooping multicast router version for a circuit.

Table 18.6 Configuring the IGMP Snooping Multicast Router Version for a Circuit

	Command Entry	Purpose
Step 1.	`8800# enable config`	Enter the configuration mode.
Step 2.	`8800(config)# ckt name pe1-to-pe3 protocol igmp-snooping mrouter v2`	Defines the multicast router IGMP version on a circuit.
Step 3.	`8800(config)# exit`	Exit configuration mode.
Step 4.	`8800 # show ckt name pe1-to-pe3 protocol igmp-snooping extensive`	Display IGMP snooping configuration for a circuit.

Configuring an IGMP Snooping Static Group on a Circuit

Table 18.7, page 4-372, lists the CLI commands to add or delete an IGMP Snooping multicast group to a circuit.

Table 18.7 Configuring a Static Group on a Circuit

	Command Entry	Purpose
Step 1.	`8800# enable config`	Enter the configuration mode.

Step 2.	`8800(config)# ckt name pe1-to-pe3 protocol igmp-snooping static-group 239.0.0.1`
	
	`8800(config)# ckt name pe1-to-pe3 protocol igmp-snooping no static-ic-group 239.0.0.1`
		Adds a multicast group (non-local class D IP address) to a circuit.
		
		OR
		
		Deletes a multicast group (non-local class D IP address) from a circuit.

Step 3.	`8800(config)# exit`	Exit configuration mode.
Step 4.	`8800 # show ckt name pe1-to-pe3 protocol igmp-snooping extensive`	Display IGMP snooping configuration for the VPLS interface.

Displaying IGMP Snooping on a VPLS Circuit

Use the **show ckt protocol igmp-snooping** command to display the IGMP snooping attributes for a VPLS circuit.

```
8800# show ckt name pe1-to-pe3 protocol igmp-snooping

                                    Op   Igmp  Imm  Static Total
Circuit          Bridge Instance    St   Ver   Lve  Group  Group
---------------- ---------------- ---  ----  ---  -----  -----
pe1-to-pe3       v1               up   V2    en   0      0

8800# show ckt name pe1-to-pe-3 protocol igmp-snooping extensive

Circuit: pe1-to-pe3; Bridging Instance: v1
  Admin State: enable; Oper Status: up; Failure Reason: none
  Immediate Leave: enable; Conf MRouterVer: none; Runtime IgmpVer: V2
  Total Groups: 0; Static Groups: 0
  Last Group Clear Time: not available; MRouter Type: dynamic; Rem Time: 299
```

Use the **show ckt protocol igmp-snooping bridging-instance groups** command to display groups assigned to a circuit for a selected bridging instance.

```
8800# show ckt name pe1-to-pe3 protocol igmp-snooping bridging-instance v1
groups all

Ckt              Group Addr       Ver  Type Remain   Last Reporter
---------        ----------       ---  ---- -------  -------------
pe1-to-pe3       239.0.0.1        V2   Dyn  149      0.0.0.0

8800# show ckt name pe1-to-pe3 protocol igmp-snooping bridging-instance v1
groups all extensive

Circuit: pe1-to-pe3
    Group: 239.0.0.1; IGMP Version: v2; Last Reporter: 0.0.0.0
    Group Type: Dynamic
    Start Time: 09/23/2009 14:01:00; Remaining Time: 208
```

Use the **show ckt protocol igmp-snooping statistics** command to display statistics for an IGMP snooping circuit.

```
8800# show ckt name pe1-to-pe3 protocol igmp-snooping statistics

Statistics Information:
  Category               Count      Category               Count
  --------               -------    --------               -------
  Tx General Query       0          Rx General Query       625
```

```
Tx Group Spec Query     0          Rx Group Spec Query     0
Tx V1 Report            0          Rx V1 Report            0
Tx V2 Report            0          Rx V2 Report            0
Tx Group Leave          0          Rx Group Leave          0
Tx Unknown Type         0          Rx Unknown Type         0
                                   Rx Error Packet         0
                                   Rx Drop Packet          0
```

USER NOTES

TELLABS DOCUMENTATION